UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

---------- x		**ELECTRONICALLY FILED**
	:	
	:	
	:	
In re SONY BMG CD Technologies Litigation	:	No. 05 CV 9575 (NRB)
	:	
	:	
	:	
---------- x		

DECLARATION OF J. SCOTT DINSDALE IN SUPPORT OF
FINAL APPROVAL OF THE SETTLEMENT

EXHIBITS C-D

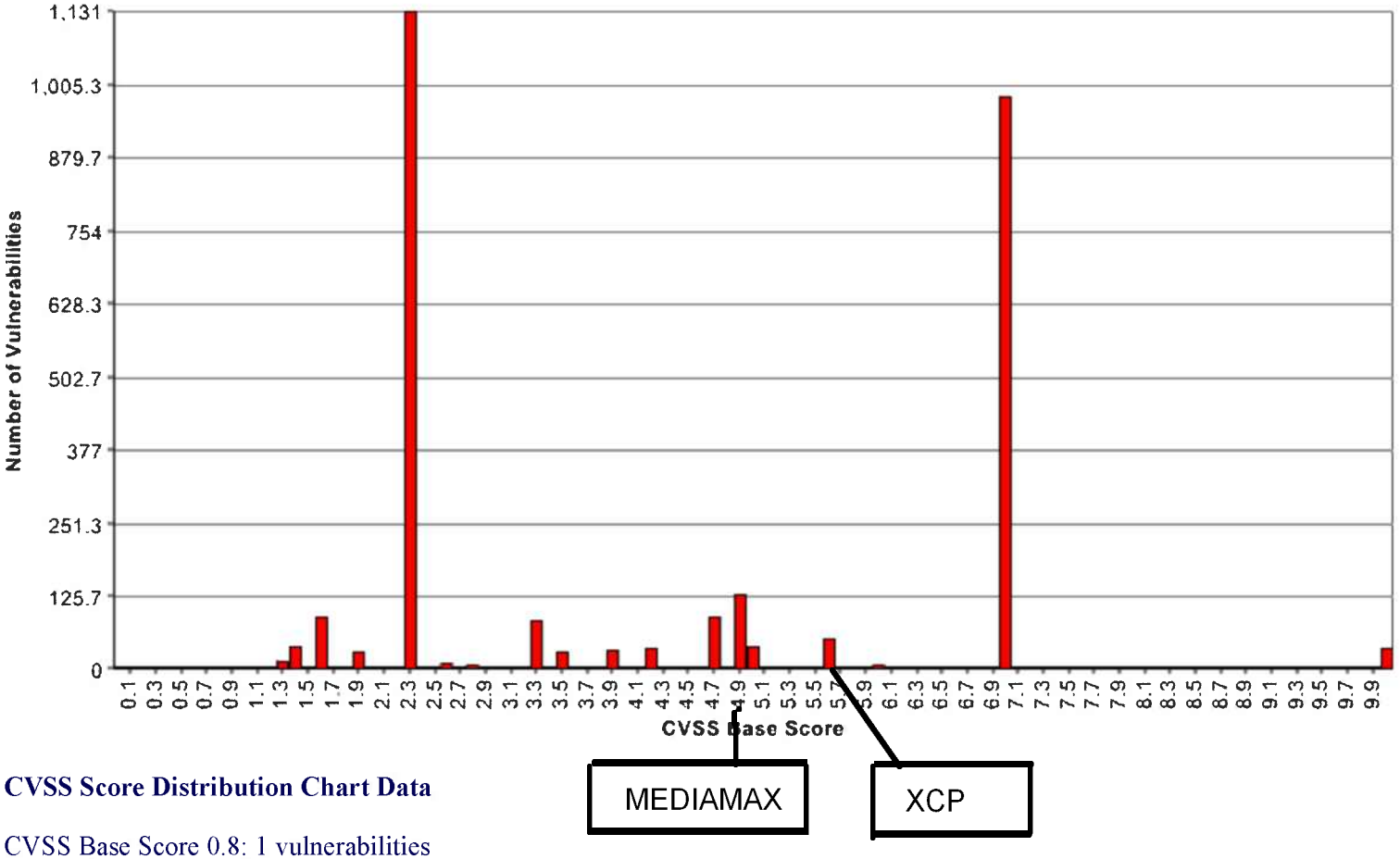
Exhibit C

NVD/CVE CVSS Vulnerability Score Distributions

This web page displays the distribution of CVSS base scores for all CVE vulnerabilities that have been fully scored within NVD. does NOT include archival CVE vulnerabilities for which the CVSS scores were approximated from partial data. This may take a minute to calculate, please be patient.

Total number of CVE vulnerabilities with CVSS base scores: 2901

CVSS Base Score Distribution for CVE Vulnerabilities



CVSS Score Distribution Chart Data

CVSS Base Score 0.8: 1 vulnerabilities
CVSS Base Score 1: 6 vulnerabilities
CVSS Base Score 1.1: 1 vulnerabilities
CVSS Base Score 1.3: 14 vulnerabilities
CVSS Base Score 1.4: 40 vulnerabilities
CVSS Base Score 1.6: 90 vulnerabilities
CVSS Base Score 1.8: 6 vulnerabilities
CVSS Base Score 1.9: 31 vulnerabilities
CVSS Base Score 2: 6 vulnerabilities
CVSS Base Score 2.3: 1131 vulnerabilities
CVSS Base Score 2.5: 3 vulnerabilities
CVSS Base Score 2.6: 10 vulnerabilities
CVSS Base Score 2.8: 7 vulnerabilities
CVSS Base Score 2.9: 5 vulnerabilities
CVSS Base Score 3: 2 vulnerabilities
CVSS Base Score 3.3: 84 vulnerabilities
CVSS Base Score 3.4: 2 vulnerabilities
CVSS Base Score 3.5: 31 vulnerabilities

CVSS Base Score 3.7: 3 vulnerabilities
CVSS Base Score 3.9: 35 vulnerabilities
CVSS Base Score 4: 3 vulnerabilities
CVSS Base Score 4.2: 36 vulnerabilities
CVSS Base Score 4.7: 92 vulnerabilities
CVSS Base Score 4.8: 1 vulnerabilities
CVSS Base Score 4.9: 128 vulnerabilities — MEDIAMAX
CVSS Base Score 5: 41 vulnerabilities
CVSS Base Score 5.2: 1 vulnerabilities
CVSS Base Score 5.3: 2 vulnerabilities
CVSS Base Score 5.6: 52 vulnerabilities — XCP
CVSS Base Score 6: 7 vulnerabilities
CVSS Base Score 6.7: 2 vulnerabilities
CVSS Base Score 7: 987 vulnerabilities
CVSS Base Score 8: 4 vulnerabilities
CVSS Base Score 10: 37 vulnerabilities

Individual CVSS Base Scores for all Fully Scored CVE Vulnerabilities

CVE-2004-2648 **CVSS Base Score: 0.8** (AV:L/AC:H/Au:R/C:N/I:N/A:P/B:N)
CVE-2003-0986 **CVSS Base Score: 1** (AV:L/AC:L/Au:R/C:N/I:N/A:P/B:N)
CVE-2006-0386 **CVSS Base Score: 1** (AV:L/AC:L/Au:R/C:P/I:N/A:N/B:N)
CVE-2006-0391 **CVSS Base Score: 1** (AV:L/AC:L/Au:R/C:N/I:P/A:N/B:N)
CVE-2006-0554 **CVSS Base Score: 1** (AV:L/AC:L/Au:R/C:N/I:P/A:N/B:N)
CVE-2006-0920 **CVSS Base Score: 1** (AV:L/AC:L/Au:R/C:P/I:N/A:N/B:N)
CVE-2006-0956 **CVSS Base Score: 1** (AV:L/AC:L/Au:R/C:N/I:N/A:P/B:N)
CVE-2002-2202 **CVSS Base Score: 1.1** (AV:L/AC:H/Au:R/C:C/I:N/A:N/B:N)
CVE-2004-2530 **CVSS Base Score: 1.3** (AV:L/AC:H/Au:NR/C:N/I:P/A:N/B:N)
CVE-2004-2541 **CVSS Base Score: 1.3** (AV:L/AC:H/Au:NR/C:N/I:P/A:N/B:N)
CVE-2005-3342 **CVSS Base Score: 1.3** (AV:L/AC:H/Au:NR/C:N/I:P/A:N/B:N)
CVE-2005-3649 **CVSS Base Score: 1.3** (AV:L/AC:H/Au:NR/C:N/I:P/A:N/B:N)
CVE-2006-0935 **CVSS Base Score: 1.3** (AV:L/AC:H/Au:NR/C:N/I:N/A:P/B:N)
CVE-2006-0926 **CVSS Base Score: 1.3** (AV:L/AC:H/Au:NR/C:N/I:P/A:N/B:N)
CVE-2006-0898 **CVSS Base Score: 1.3** (AV:L/AC:H/Au:NR/C:P/I:N/A:N/B:N)
CVE-2006-0741 **CVSS Base Score: 1.3** (AV:L/AC:H/Au:NR/C:N/I:N/A:P/B:N)
CVE-2006-0836 **CVSS Base Score: 1.3** (AV:L/AC:H/Au:NR/C:N/I:N/A:P/B:N)
CVE-2006-0591 **CVSS Base Score: 1.3** (AV:L/AC:H/Au:NR/C:P/I:N/A:N/B:N)
CVE-2006-0641 **CVSS Base Score: 1.3** (AV:L/AC:H/Au:NR/C:P/I:N/A:N/B:N)
CVE-2006-0050 **CVSS Base Score: 1.3** (AV:L/AC:H/Au:NR/C:N/I:P/A:N/B:N)
CVE-2006-1066 **CVSS Base Score: 1.3** (AV:L/AC:H/Au:NR/C:N/I:N/A:P/B:N)
CVE-2006-1231 **CVSS Base Score: 1.3** (AV:L/AC:H/Au:NR/C:N/I:P/A:N/B:N)
CVE-2006-1270 **CVSS Base Score: 1.4** (AV:R/AC:L/Au:R/C:N/I:P/A:N/B:N)
CVE-2006-1281 **CVSS Base Score: 1.4** (AV:R/AC:L/Au:R/C:N/I:P/A:N/B:N)
CVE-2006-1119 **CVSS Base Score: 1.4** (AV:R/AC:L/Au:R/C:P/I:N/A:N/B:N)
CVE-2006-1147 **CVSS Base Score: 1.4** (AV:R/AC:L/Au:R/C:N/I:N/A:P/B:N)
CVE-2006-1383 **CVSS Base Score: 1.4** (AV:R/AC:L/Au:R/C:P/I:N/A:N/B:N)
CVE-2006-1387 **CVSS Base Score: 1.4** (AV:R/AC:L/Au:R/C:N/I:N/A:P/B:N)
CVE-2006-1510 **CVSS Base Score: 1.4** (AV:R/AC:L/Au:R/C:N/I:P/A:N/B:N)
CVE-2006-1540 **CVSS Base Score: 1.4** (AV:R/AC:L/Au:R/C:N/I:N/A:P/B:N)
CVE-2006-0127 **CVSS Base Score: 1.4** (AV:R/AC:L/Au:R/C:N/I:P/A:N/B:N)
CVE-2006-0172 **CVSS Base Score: 1.4** (AV:R/AC:L/Au:R/C:N/I:P/A:N/B:N)
CVE-2006-0173 **CVSS Base Score: 1.4** (AV:R/AC:L/Au:R/C:N/I:P/A:N/B:N)
CVE-2006-0174 **CVSS Base Score: 1.4** (AV:R/AC:L/Au:R/C:P/I:N/A:N/B:N)
CVE-2006-0309 **CVSS Base Score: 1.4** (AV:R/AC:L/Au:R/C:N/I:N/A:P/B:N)
CVE-2006-0340 **CVSS Base Score: 1.4** (AV:R/AC:L/Au:R/C:N/I:N/A:P/B:N)
CVE-2006-0354 **CVSS Base Score: 1.4** (AV:R/AC:L/Au:R/C:N/I:N/A:P/B:N)
CVE-2005-4449 **CVSS Base Score: 1.4** (AV:R/AC:L/Au:R/C:N/I:P/A:N/B:N)
CVE-2005-4625 **CVSS Base Score: 1.4** (AV:L/AC:H/Au:NR/C:N/I:C/A:N/B:A)
CVE-2005-4740 **CVSS Base Score: 1.4** (AV:R/AC:L/Au:R/C:N/I:N/A:P/B:N)
CVE-2006-0657 **CVSS Base Score: 1.4** (AV:R/AC:L/Au:R/C:N/I:P/A:N/B:N)
CVE-2006-0424 **CVSS Base Score: 1.4** (AV:R/AC:L/Au:R/C:P/I:N/A:N/B:N)

Exhibit D

cybertrust

SONY BMG

Privacy Assessment

March 30, 2006: Version 2.1

www.cybertrust.com

13650 Dulles Technology Dr. Suite 500
Herndon, VA 20171-4602

703.480.8200

Table of Contents

1 Executive Summary

Cybertrust was engaged by SONY BMG Entertainment, Inc. ("SONY BMG") to determine whether SONY BMG used XCP or MediaMax content protection software to collect, aggregate, or retain individuals' personal information without their express consent. The purpose of the engagement was to confirm representations by SONY BMG, as set forth in a Settlement Agreement in In re SONY BMG CD Technologies Litigation, No 1:05-cv-09575 (NRB) (S.D.N.Y., preliminarily approved, Jan. 6, 2006).

For the engagement, Cybertrust interviewed personnel of SONY BMG and SunnComm International Inc. ("SunnComm"), as well as of Stroz Friedberg, LLC, SONY BMG's data security and computer forensics experts, analyzed CDs protected by XCP and MediaMax software, and conducted on-the-console inspection of SONY BMG and SunnComm systems.

Cybertrust concludes that the XCP and MediaMax software, which includes the XCP Bundled Player, and the MediaMax v.3 and MediaMax v.5 Players, only collect non-personal information tied to a particular album and its usage. This information is collected for two specific purposes:

1. to deliver a more personalized user experience through the delivery of album specific content, and
2. to ensure that rules applicable to the usage of the music content on the CDs are enforced.

In connection with the first of these purposes, if the user's computer has a live Internet connection, the XCP and MediaMax Players communicate only:

a) the unique album ID ("uId" for XCP CDs, "id" and "hackID" for MediaMax CDs) or song ID ("CID" for MediaMax only), and

b) the IP address of the user's Internet connection.

The unique album ID is used to return to the user's player content and, in the case of MediaMax v. 3 titles, license information specific to the CD title.

Cybertrust did not find any evidence that SONY BMG used the XCP Software or that SunnComm used the MediaMax Software, or that any of the enhanced content on XCP CDs or MediaMax CDs was used, to collect, aggregate, or retain information that could be identified with or tracked to an individual without such person's express consent.

2 Scope & Facts

Cybertrust was engaged to determine if SONY BMG collected, aggregated, or retained Personal Data in a manner that is inconsistent with the following representations ("SONY BMG Representations").

2.1 SONY BMG Representations

SONY BMG asserts that it has not used the MediaMax or XCP Software, or any of the enhanced content on the XCP CDs or MediaMax CDs, to collect, aggregate or retain Personal Data about persons who listened to XCP CDs or MediaMax CDs on computers, without such person's express consent. SONY BMG further asserts that it only has collected information necessary to provide enhanced CD functionality. SONY BMG believes, and on that basis asserts, that such functionality requires that the album title, artist, IP address, and certain non-personally identifiable information be collected. Beginning prior to the Fairness Hearing, SONY BMG will take commercially reasonable steps to destroy the information it collects to provide enhanced CD functionality, including logs of IP addresses, within ten (10) days after the collection of such data, except as required by law, regulation, litigation discovery rule or court order. SONY BMG shall, however, be permitted to compile aggregate, non-personally identifiable data about hits to its servers from enhanced CDs.

For purposes of the SONY BMG Representations and Cybertrust's assessment, the following terms have the following definitions:

"Enhanced CDs" or "Connected CDs" are audio CDs that, upon being loaded into a personal computer, initiate connections over the Internet to a server for the purpose of allowing the server to provide information to the user interface regarding the artist or the music on the CD (the "Enhanced CD Functionality").

"MediaMax CDs" are audio CDs that contain a version of MediaMax Software.

"MediaMax Software" means "MediaMax" content protection software used in connection with certain audio CDs released by SONY BMG and one of its predecessors, BMG, and includes MediaMax version 3.0 and MediaMax version 5.0.

"Personal Data" means information stored on a computer that itself discloses the identity of the individual using that computer or websites, other than the SONY BMG and SunnComm websites, that the user has visited using the browser on such computer, but does not include the IP address of the computer's Internet connection or any information with respect to an album title, artists and tracks, or other non-personally identifiable information, that is routinely logged by SONY BMG in connection with Enhanced or Connected CDs.

"XCP CDs" are audio CDs that contain XCP Software.

"XCP Software" means the "XCP" content protection software used in connection with certain audio CDs released by SONY BMG commencing in Spring 2005.

The Fairness Hearing refers to the hearing at which the court will consider the proposed settlement, as set forth in the Settlement Agreement in *In re SONY BMG CD Technologies Litigation*, No 1:05-cv-09575 (NRB) (S.D.N.Y., preliminarily approved, Jan. 6, 2006).

2.2 Platforms

Cybertrust's assessment of the XCP and MediaMax software was limited to the Windows operating system[1].

2.3 Applications

Three applications are within the scope of Cybertrust's assessment:

- XCP Bundled Player
- MediaMax v.3 Player
- MediaMax v.5 Player

Each of these three player applications allows an end user to play music contained on a XCP CD or MediaMax CD, as the case may be, on a computer, as well as to copy (or "rip") tracks to the computer's hard drive. Both the XCP Bundled Player and the MediaMax v.5 Player also enable the creation of a limited number of personal CD-R copies ("burns"). The following sections describe those disc operations that collect, communicate, and store data (of any type) to provide the Enhanced CD Functionality.

XCP Bundled Player

When an XCP CD is inserted into a user's computer for the first time, the user is visually presented with an End User License Agreement ("EULA") to which the user must agree to access the media on the CD. If the user does not accept the EULA, the CD is ejected from the computer ROM drive.

Once a user has agreed to the terms of the EULA, registry entries are created by the XCP application on the computer hard drive to reflect the user's acceptance for that specific title. The actual values assigned to the "InstallRevisionHi" and "InstallRevisionLo" registry keys reflect the version of the XCP Software specific to the XCP CD a user is listening to and are not tied to the user or a user's activity. The version number is noted in order to prevent older versions of the XCP Software from being installed.

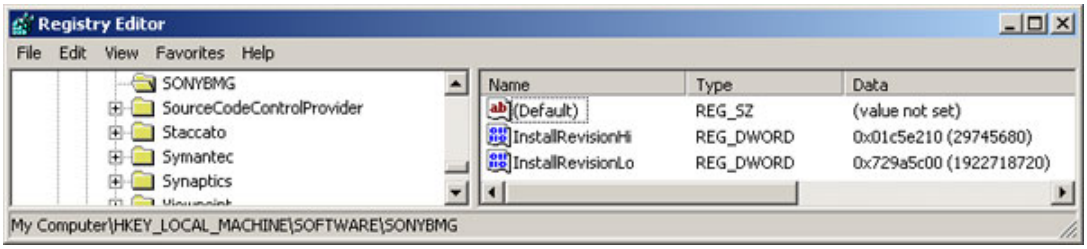


Figure 2-1

Subsequent to the user's acceptance of the EULA, the XCP CD will perform a one-time installation of XCP Software onto the hard drive, following which the XCP Bundled Player will run in the computer's volatile memory.

[1] XCP CDs do not include software for the Macintosh platform, while MediaMax CDs do not protect the audio and offer only limited enhanced CD functionality on the Macintosh platform.

The XCP Bundled Player application checks whether a connection is available to the Internet. If so, the XCP Bundled Player application makes a one-time call per session to SONY BMG's server environment to check for and request additional content. If content is available, the server sends an XML file that contains the location of the content (i.e. banner(s)), the rotation interval for that content, as well as web links that a user's web browser would be directed to if they clicked on a particular banner. The banners are rotated within the XCP Bundled Player until the player is closed or the volatile memory is flushed (i.e. a system reboot or power loss to the system).

The XCP Bundled Player application does not make any additional calls to the Internet after the one-time call noted above has been completed, regardless of its success or failure.

The XCP Bundled Player application allows users to create up to three copies (or "burns") of the music content on an XCP CD. The user is prevented from making more than three burns by a counter. The counter is maintained within an encrypted file on the user's hard drive (%windir%\system32\$sys$filesystem\$sys$parking). Upon each successful burn, the counter is appropriately updated to prevent the user from burning more than the authorized limit of three copies.

MediaMax v.3 Player

When a MediaMax CD is inserted into a user's computer for the first time, the user is visually presented with a EULA to which the user must agree to access the content on the CD. If the EULA is not accepted, the CD is ejected from the computer ROM drive. Upon user acceptance of the EULA, the MediaMax v.3 Player reflects the user's acceptance of the EULA within an encrypted ".dat" file that is written to the user's computer hard drive. After acceptance of the EULA and installation of the MediaMax Software, the MediaMax v.3 Player will check for a connection to the Internet, and if a connection exists, the MediaMax software will attempt an outbound connection to license.sunncomm2.com to obtain Microsoft DRM v1 license information in order to support media players that do not support Microsoft DRM v7 licenses[2]. This is a onetime only request. License information, either on the MediaMax v. 3 CD or online, are needed to play the contents of the CD and to provide access to pre-ripped, encrypted Windows Media Audio (WMA) files that are contained in the data (second) session of MediaMax v.3 CDs. The licensing mechanism adheres to the standards that define the architecture for Microsoft's DRM deployment.

MediaMax v.5 Player

When a MediaMax v.5 CD is inserted into a user's computer, the user is visually presented with a EULA to which the user must agree to access the content on the CD. If the EULA is not accepted, the CD is ejected from the computer ROM drive. Similar to the MediaMax v.3 Player, the MediaMax v.5 Player reflects the user's acceptance of the EULA within an encrypted ".dat" file that is written to the user's computer hard drive.

The MediaMax v.5 Player, unlike the MediaMax v. 3 Player, does not need to obtain license information, either on the MediaMax CD or online, to play the contents of the CD. License information is needed only when the user wishes to rip the music from the CD to the hard drive of the computer. Unlike the MediaMax v.3 CDs, the MediaMax v.5 CDs do not come packaged with WMA files. When a user rips the music from a MediaMax v. 5 CD to the hard drive of the computer, secure WMA files are created on the computer and pre-packaged Microsoft DRM v.7 license information is transferred to the user's computer hard drive.

[2] CDs with MediaMax v.3 software come prepackaged with Microsoft DRM v.7 licenses.

The MediaMax v.5 Player also contains the Perfect Placement feature, which determines if an Internet connection is available when a user attempts to use a MediaMax v.5 CD. If a connection to the Internet is available, the application will contact SunnComm's server environment and submit a request for additional content. The SunnComm server sends an XML file that contains the number of banner ads available, the banners themselves, the rotation interval for the banners, as well as web links that a user's web browser would be directed to if they clicked on a particular banner.

If an Internet connection is not available, the application will continue to check for a connection to the Internet every minute until the CD is no longer being used, or until a connection becomes available (upon which it will execute the process of pulling banner content from the SunnComm server).

The MediaMax v.5 Player allows users to create limited burns of the MediaMax v.5 CD. The user is prevented from making more than the permitted number of burns by a counter. The counter is maintained within the same encrypted ".dat" file that is written to the user's computer hard drive when the user accepts the EULA. Upon each successful burn, the counter is appropriately updated to ensure that the user is prevented from burning more than the authorized number of copies.

Promo Play (Tune Share)

Both the MediaMax v.3 and MediaMax v.5 Players send data from the user's computer to SunnComm when a user affirmatively chooses to take advantage of the Promo Play (alternatively called TuneShare) feature that is provided within the MediaMax application. Promo Play allows a user to select songs on a MediaMax CD that the user would like his or her friends to sample. Through the MediaMax application, the user supplies information (e.g. name of the song, email address of a friend) and generates an email for forwarding to the intended recipient. When a Promo Play (TuneShare) email is submitted through the MediaMax Software, the information volunteered by the sender in the name and email fields for both the sender and receiver, the text added to the message field by the sender, and the CID of the song being shared are communicated by the MediaMax Software to SunnComm's Promo Play server. SunnComm's Promo Play server takes the request and creates an email that contains an embedded link and forwards the message on to the recipient email address provided by the sender. If the recipient wishes to access the music that the user wished to share, the recipient must click the embedded link. When the recipient clicks the embedded link, a call is made to the license.sunncomm2.com server to obtain the appropriate license information to enable the recipient to play the shared song, followed by a protected version of the song itself. The licensing mechanism adheres to the standards that define the architecture for Microsoft's DRM deployment. As Promo Play is a feature enabled solely through the express consent of the user of the MediaMax v. 3 and MediaMax v. 5 Players, SONY BMG has deemed it as outside the scope of this assessment by Cybertrust.

2.4 Servers

Cybertrust reviewed the servers associated with the following domains, which were identified as supporting the XCP Bundled Player, the MediaMax v.3 Player, and the MediaMax v.5 Player:

- www.sonymusic.com
- access.sonymusic.com
- connected.sonymusic.com
- xcpimages.sonybmg.com
- license.sunncomm2.com

Cybertrust also reviewed the following systems, which participate in the transfer or storage of data tied to the XCP Bundled Player, the MediaMax v.3 Player, or the MediaMax v.5 Player:

- XCP Player
  - ConnecteD Web Cluster
  - DFS Application Cluster
  - Oracle DB Cluster
- MediaMax v.3 and MediaMax v.5 Players
  - HUGO
  - SUNNY
  - License1
  - SUNNWEB

Cybertrust conducted interviews and on-console reviews to identify sources of evidence, such as log files, back-up files and databases. Cybertrust's assessment included reviews of sources of evidence within the scope of the project that were used to quantify the resident data. Cybertrust reviewed these sources to determine whether SONY BMG and SunnComm complied with the SONY BMG Representations.

3 Methodology

3.1 Provided Materials

During the assessment, SONY BMG and SunnComm provided Cybertrust with a variety of information in both electronic and hard copy formats. Cybertrust interviewed key SONY BMG and SunnComm personnel regarding their roles, the applications and systems under assessment, relevant information flow, and the structure of the organizations' infrastructure.

More specifically, Cybertrust was provided the following:

SONY BMG:

- Log samples from the ConnecteD web cluster
- Database Schema information from the Oracle DB cluster
- Database export from logging table within the Oracle DB cluster
- XCP Bundled Application Source Code
- XCP Bundled Application flow chart
- XCP database decrypter
- Patty Loveless (dreamin' my dreams) XCP CD
- Dave Matthews Band (Stand Up) MediaMax v.3 CD
- Raheem DeVaughn (The Love Experience) MediaMax v.5 CD

SunnComm

- Database exports from relevant tables
- Web logs
- Network diagram
- Unencrypted Counter File

3.2 Tools

Cybertrust used the following commercial and open source tools to perform a handful of primary tasks:

1. Data Packet Capture / Analysis
2. Log Analysis
3. Data Base Analysis
4. System Imaging / Deployment
5. Testing Process Management

3.2.1 Data Packet Capture / Analysis

The purpose of Data Packet Capture / Analysis tools is to record all traffic that passes through a specified network interface. Traffic is captured in a manner that allows the assessor to comprehensively review the low level anatomy of network communications. Specific to this assessment, Ethereal – Network Protocol Analyzer Version 0.10.12 was used with WinPcap version 3.1 beta4.

As a standard, Ethereal – Network Protocol Analyzer was configured to capture and read network traffic in its entirety, i.e. promiscuous mode. Performing a data packet capture and analysis in promiscuous mode enables the assessor the opportunity to intercept and assess each ingress and egress network packet that passes through a target interface.

Capture sessions were created in accordance with testing scenarios and followed the naming standard:

- ApplicationName_ScenarioNumber. = > XCP_Scenario1

3.2.2 *Log Analysis*

Log analysis tools were utilized to expedite the process of analyzing log files, which in many cases come in the form of delimited flat files. Log analysis tools allow assessors flexible searching and sorting capabilities.

Cybertrust analyzed logs of exports from web, application, and database servers on the Windows and Solaris operating environments.

Two log analysis tools were used to assess the log exports from the in-scope systems:

- Microsoft's Logparser v2.2
- Cygwin v1.5.19-4 (GREP – general regular expression parser)

3.2.3 *Database Analysis*

In addition to evidence sources sitting within flat files, in-scope systems housed relevant information within Oracle and SQL Server databases.

To confirm that personally identifiable information was not being collected, aggregated, or retained, without express user consent, Structured Query Language (SQL) was used to poll the contents of both the Oracle and SQL Server databases, to pull database schema and content, and to validate the nature of such data.

3.2.4 *System Imaging / Deployment*

Effectively testing a set of conditions requires the existence of technical controls to hedge against the risk to the integrity of the test results by variables such as configuration parameters. A standard test host was developed and imaged using a system imaging tool. This standard test image was used throughout the entire testing process to ensure that the test results would not be impacted by differences in configuration that could come as a result of the testing process or from using different test hosts.

Symantec Ghost Version 8.0.0.984 was the imaging and deployment tool used to create and deploy a standard environment across the test scenarios for the XCP Bundled Player and the MediaMax v.3 and MediaMax v.5 Players.

3.2.5 *Testing Process Management*

Cybertrust used process controls in the form of a testing program that served as a means of ensuring that the results are repeatable and that the testing methodology lends itself to replication, accurate measurement, and acceptability.

The testing methodology employed by Cybertrust helped ensure that the assessment covered the appropriate test scenarios and that the actual tests were run in a fashion that would allow the assessors to have the most complete view of the way data is handled by the XCP and MediaMax Software.

3.3 Assessment Execution

The methodology used by Cybertrust to carry out the engagement relied on the people that were interviewed, the information that was reviewed, the tools that were used, and the processes that were specifically developed for the assessment.

Different tools, people, and processes were involved throughout the life of the assessment and the extent to which any tool, person, or process participated in the assessment was determined from the information taken from interviews with SONY BMG and SunnComm, as well as documentation provided by both SONY BMG and SunnComm.

The testing program was developed specifically to quantify the flow of data in and out of the in-scope applications using the data packet capture and analysis tools.

Prior to completing the testing program, log and database analysis tools were used to review the servers associated with the XCP, MediaMax v.3 and MediaMax v.5 Software. This pre-testing assessment was undertaken to determine the degree to which pre-existing data provide insight into SONY BMG and SunnComm's adherence to the SONY BMG Representations.

After SONY BMG and SunnComm's adherence to the SONY BMG Representations was evaluated through the successful execution of the testing program, the data residing within the in-scope servers were reexamined by analyzing the retention of any new data generated during the course of the assessment.

4 Detailed Findings

Cybertrust's detailed findings can be divided into the client side privacy assessment and the server side privacy assessment.

On the client side, Cybertrust assessed the innate capabilities of the XCP, MediaMax v.3 and MediaMax v.5 Software to collect, communicate, and store data (of any type) to provide the Enhanced CD Functionality.

On the server side, Cybertrust assessed the web, application, and database servers that support the functionality of the client-side applications, including the transport and storage of any data communicated by the client applications to the server segments.

4.1 Client Side Privacy Assessment

The client applications were the primary focal point of Cybertrust's assessment because Cybertrust concluded that determining the data handling capabilities of those applications would provide the most relevant information regarding SONY BMG's and SunnComm's adherence to the SONY BMG Representations.

The granular details that drove the client side privacy assessment for the three applications can be found in Appendix 1 of this document.

4.1.1 XCP Bundled Player

Cybertrust's assessment of the XCP Bundled Player involved the complete testing of all the capabilities of, or delivered through, the XCP Bundled Player, including:

- Playing the music on the XCP CD
- Presenting value added content to the user through the display of album specific content in the form of rotating banners
- Ripping the contents of the XCP CD to the hard drive
- Burning multiple copies of the music on the XCP CD.

Cybertrust observed that when an XCP CD is initially loaded into a computer for the first time, the XCP Bundled Player initializes and runs in the computer's RAM. If an Internet connection is available, the XCP Bundled Player will make an outbound call to connected.sonymusic.com with a request for banner content specific to the album being played. To ensure that the banners that are pulled down correctly align with the artist / album being played on the XCP CD, the XCP Bundled Player sends along with its initial communication with connected.sonymusic.com a unique ID (a.k.a. uId), which is used to uniquelyidentify albums, in addition to certain redirect links, and other content-centric materials on SONY BMG's servers. The use of a unique ID permits the same ID to be communicated to connected.sonymusic.com regardless of which computer or which user plays the CD.

When a user inserts a XCP CD into his or her computer, the XCP Bundled Player will make an outbound request to connected.sonymusic.com with the "uId". In response to the "uId", the SONY BMG server (connected.sonymusic.com) sends back to the XCP Bundled Player a link to an xml file stored on the xcpimages.sonybmg.com server. The XCP Bundled Player follows the link to the xml file on xcipimages.sonybmg.com to pull down an XML file with parameters that define how the banner on the XCP Bundled Player should operate.

Figure 4-1

The XML file specifies which banners to display on the user's XCP Bundled Player, from where the specific banner file can be downloaded, what address to link to each banner, and how long to display each banner.

When a user clicks on any of the downloaded banners, the XCP Bundled Player opens a web browser, if one is not already open, and redirects the browser to the web addressed linked to the banner. If a browser is already opened, the XCP Bundled Player will redirect the active web browser to the web addressed linked to the banner.

Cybertrust determined that the XCP Bundled Player maintains an encrypted database on the user's computer. The purpose of the database is to enforce usage limitations applicable to particular activities on a particular computer, in particular, to ensure that the user is not able to burn a CD in excess of the allowed limits

The database that maintains the usage permissions and counter is an encrypted text file. Cybertrust decrypted the file to assess if it enabled SONY BMG to collect or aggregate personally identifiable information, regardless of whether such information was communicated to SONY BMG (or any other person). The encrypted database maintains information on individual tracks within an album. For each track, the database maintains the Record # and GUID, as well as its usage, which takes on the values:

- Plays
- Copy to CD
- Copy to Hard Disk
- Copy to Portable Device
- Network Checkout

Within a specific type of usage, such as USAGE = PLAYS, the database maintains the same five parameters:

- Count

- Territory
- Days to Expiry
- Expiry Start
- Expiry End

Figure 4-2

Cybertrust confirmed that the contents of the database file, when unencrypted, are constants that are tied to content usage variables that are referenced to usage rules set forth in the EULA. Cybertrust confirmed that only usage information, as it pertains to CD content usage permissions, was captured and maintained. Accordingly, the database has no capability to associate a specific individual to the usage recorded within the database.

The XCP Player also records the user's acceptance of the EULA. This record is not encrypted nor is acceptance or rejection of the EULA communicated by the XCP Bundled Player or otherwise from the user's computer.

The XCP Player additionally makes multiple writes to the system registry. Of the registry keys that are written to the end user's computer hard drive, two keys reflect information specific to the most recent CD played.

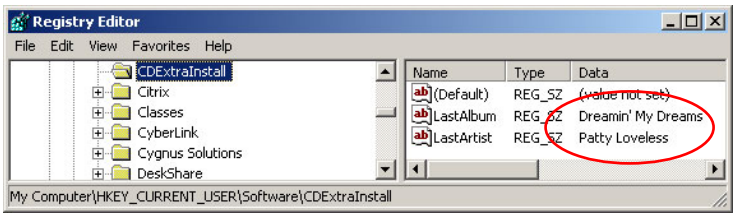


Figure 4-3

The assessment of the data written in the registry confirms that the information is content specific, and there is no evidence that this information is communicated from the user's computer.

Cybertrust's tests of the XCP Bundled Player's ripping and burning functions showed no signs of associated network traffic during normal operations. Nor was any information regarding usage in excess of permitted usage, such as multiple rips, beyond the authorized limits or attempts to make a number of CD copies in excess of what is allowed, communicated from the user's computer.

4.1.2 MediaMax v.3 Player

Cybertrust's assessment of the MediaMax v.3 Player involved the complete testing of all the capabilities of, or delivered through, the MediaMax v.3 Player, including:

- Playing the music on the MediaMax v. 3 CD
- Presenting album specific content through statically embedded content and links within the player
- Ripping the contents of the MediaMax v.3 CD to the hard drive

Upon loading the MediaMax v.3 CD into a machine, the MediaMax v.3 Player attempts to connect to license.sunncomm2.com/perfectplacement/online.asp?tm=1142451905993. According to SunnComm personnel, this call appears on MediaMax v.3 discs authored after June, 2004. The call contains no personal information[3]. The response that is sent back to the browser that requests the specified link is either "online=true&timing=3000&view=2" or "online=true&timing=10000&view=1". To assess how unique the response is to the input value, Cybertrust manually manipulated the link in the following manners with the associated results:

- http://license.sunncomm2.com/perfectplacement/online.asp?tm=1142451905993
  - online=true&timing=10000&view=1
- http://license.sunncomm2.com/perfectplacement/online.asp?tm=1142451905995
  - online=true&timing=3000&view=2
- http://license.sunncomm2.com/perfectplacement/online.asp?tm=1142451905996
  - online=true&timing=10000&view=1
- http://license.sunncomm2.com/perfectplacement/online.asp?tm=1142451905997
  - online=true&timing=3000&view=2
- http://license.sunncomm2.com/perfectplacement/online.asp?tm=0
  - online=true&timing=10000&view=1
- http://license.sunncomm2.com/perfectplacement/online.asp?tm=1
  - online=true&timing=3000&view=2

[3] The value that follows the "tm=" is generated by the MediaMax v.3 Player from the content on the CD.

It appears from the testing that there are only two possible responses to the outbound communication made by the MediaMax v.3 application when the CD is loaded into the user's computer; regardless of the value entered after tm=, the result will alternate between online=true&timing=10000&view=1 and online=true&timing=3000&view=2. Further investigation indicates that the communication's nature is ancillary and does not play a role in the operation of the MediaMax v.3 software.

.

MediaMax v.3 includes Microsoft DRM v.7 license information on the disc. In order to support audio playback on media players that only support v.1 of the DRM, the MediaMax v. 3 Software attempts to connect to SunnComm's licensing server in order to pull v.1 license information by sending the hackID, which is a unique non-personally identifiable value that tells the SunnComm license server which pieces of license information to send back to the client.

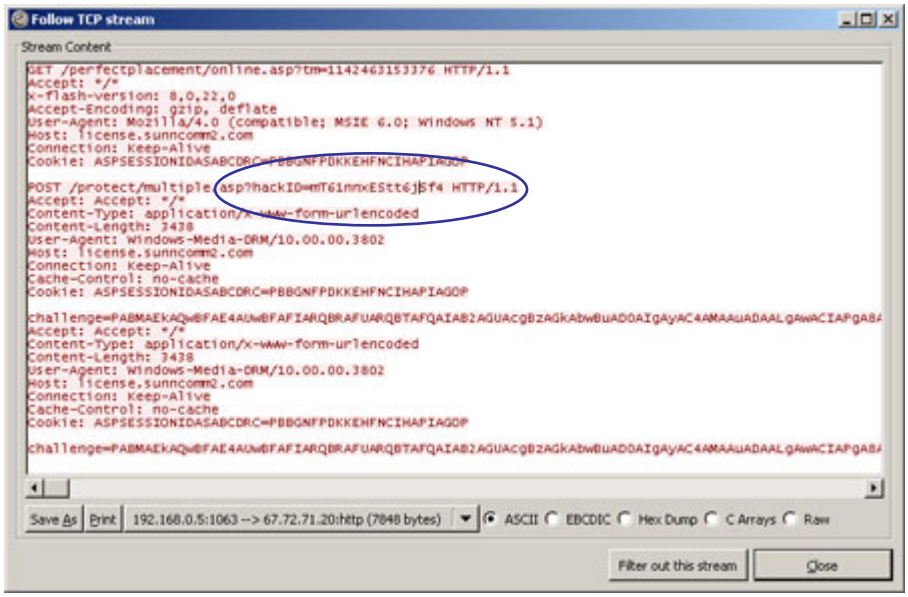


Figure 4-4

The response from the SunnComm license server to the request for license information is license information, indicated by their <LICENSERESPONSE> tags.

Tests of the MediaMax v.3 Player's ripping functions showed no signs of associated network traffic during normal operations. Nor was any information regarding usage in excess of permitted usage, such as multiple rips, beyond the authorized limits.

4.1.3 MediaMax v.5 Player

Cybertrust's assessment of the MediaMax v.5 Player involved the complete testing of the capabilities delivered through the MediaMax v.5 Player, including:

- Playing the music on the MediaMax v.5 CD
- Presenting value added content to the user through the display of album specific content in the form of rotating banners

- Ripping the contents of the MediaMax v.5 CD to the user's hard drive
- Burning multiple copies of the music on the CD

When a user inserts a MediaMax v.5 CD into his or her computer, the MediaMax v.5 Player will make an outbound request to SunnComm, sending along an album's unique ID, known as an "id". If a banner associated with the "id" is available, the server sends an HTML file with parameters that define how the banner on the MediaMax v.5 Player should operate

Figure 4-5

The HTML file specifies which banners to display on the user's MediaMax v.5 Player, from where the specific banner file can be downloaded, what address to link to each banner, how long to display each banner, and the banner's graphic type.

When a user clicks on any of the downloaded banners, the MediaMax v.5 Player sends a request to perfect.sunncom.com/default.asp with a query string that is translated on the server side to direct the client's browser to the correct web address. The query string, which looks similar to "perfectid=12345", is associated with a specific album, not an individual user.

The MediaMax v.5 Player retains an encrypted database within the user's computer to ensure adherence to the usage rules.

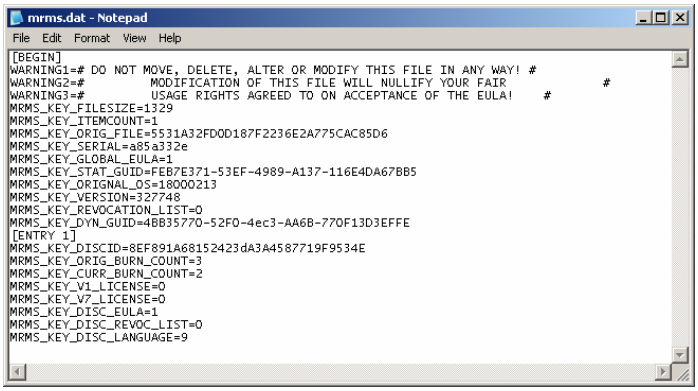


Figure 4-6

The contents of the database file, when unencrypted, are constants that are tied to the content usage variables that are referenced to usage rules set forth in the EULA. Cybertrust confirmed that only usage information, as it pertains to CD content usage permissions, was captured and maintained. Accordingly, the database has no capability to associate a specific individual to the usage recorded within the database.

Cybertrust's tests of the MediaMax v.5 Player's ripping and burning functions showed no signs of associated network traffic during normal operations. Nor was any information regarding usage in excess of permitted usage, such as multiple rips, beyond the authorized limits or attempts to make a number of CD copies in excess of what is allowed, communicated from the user's computer.

4.2 Server Side Privacy Assessment – XCP Software

The scope of the XCP Server Side Privacy Assessment was limited to those SONY BMG systems that facilitate the transfer or storage of data resulting from use of an XCP CD. Specifically, the systems that were considered in-scope are the following systems outlined below.

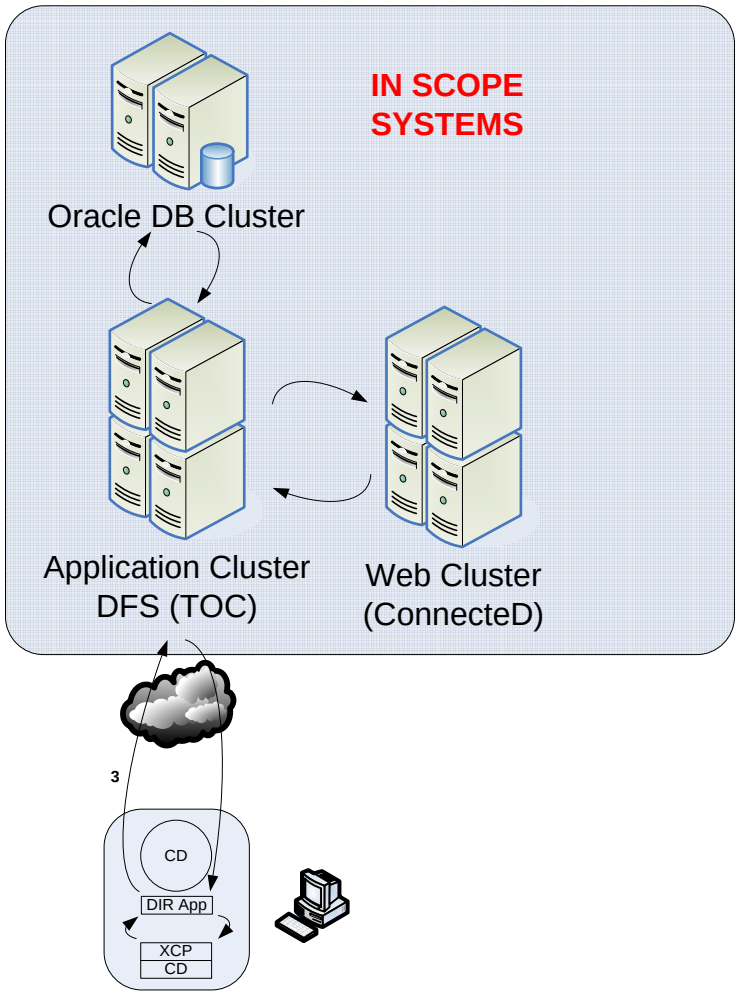


Figure 4-7

The in-scope systems are logically a set of web, application, and database servers. The logical systems represent a clustered environment, which comprises:

- A Sun Solaris v8 Cluster of Apache v1.3.27 web servers
- A Weblogic Cluster of application servers
- A cluster of Oracle 9i database servers

Within these specific clusters, Cybertrust identified and analyzed the following sources of evidence:

- Web Cluster:
  - ConnecteD Logs: The ConnecteD Logs record the initial requests from the XCP Bundled Player to the ConnecteD server for the appropriate redirect link. The redirect

links are specific to the CD being played by the client. Logs tied to the connected.sonymusic.com domain are aggregated into the ConnecteD Logs.

- Access Logs: The Access Logs record activity around the provision of the XML link that specifically maps to the artist on the CD being played by the client. Logs tied to www.sonymusic.com, access.sonymusic.com, and xcpimages.sonybmg.com are centrally stored within access logs.

- Application Cluster: The Weblogic application server, which hosts the TOC application, maintains several different sets of log files, which were all reviewed for personally identifiable data. Specifically, the following log files were reviewed.[4]
  - Pearljam_server_1_fs.log
  - Pearljam_server_1_fsadmin.log
  - Pearljam_server_1_pj.log
  - Pearljam_server_psadmin.log
  - Pearljam_server_sspromo.log
  - Toc-2006-02-07.log
  - Toc-2006-03-02.log
- Database Cluster: Activity tied to the ConnecteD-TOC authentication that is used to store the unique ID of the redirect URL sits within the CONN_REQUEST table of the Oracle database cluster.[5]
  - CONN_REQUEST

CONN_REQUEST
CONN_REQUEST_ID CONN_REQUEST_DATE CONN_REQUEST_UID CONN_REQUEST_TYPE CONN_REQUEST_SUCCESS CONN_REQUEST_SEL_NUMBER

    - CONN_REQUEST is composed of the following columns:
      - CONN_REQUEST_ID: The primary key of the table. [A sequentially assigned number]
      - CONN_REQUEST_DATE: The date of the request.
      - CONN_REQUEST_UID: The unique ID of the redirect URLs
      - CONN_REQUEST_TYPE: The type of request, either “redirect” or “connected” where XCP is represented by a “redirect” value
      - CONN_REQUEST_SUCCESS: Was the request a success? All requests reviewed within a one-week period (02/27/06 – 03/06/06) showed the value “y” for yes.
      - CONN_REQUEST_SEL_NUMBER: The selection id of the album.

The data sources showed no signs of collecting, aggregating or storing personally identifiable data. The only information which is exported from the client system that can be identified in any of the in-scope

[4] The log files reviewed on the Application Cluster authoritatively represent all of the log files generated for the TOC application.

[5] The table within the database was identified by assessing the database access granted to the application pool within which the TOC application sits.

systems on the server side are the “uId”, which (as noted) is used solely to deliver banners based on content IDs, as well as the client’s IP address, which is obtained in accordance with standard web communication protocols.

4.3 Server Side Privacy Assessment – SONY BMG Data Retention

Interviews with SONY BMG’s system administrator revealed that at the time of this assessment SONY BMG did not have a formal data retention policy governing the collection, storage, or destruction of data. SONY BMG’s current operational retention period varies across platforms, but in-scope logs, specifically web logs that maintain IP addresses, are rotated between 5 – 10 days. The maximum retention window for raw web logs is 10 days. This window is driven by hard drive storage limitations rather than a formal data retention policy.

The web logs that maintain IP addresses are rolled up into a reporting tool that provides web server statistics. A review of the statistics page showed that the information that is correlated by the reporting tool is comprised of non-personally identifiable information. Of the various types of reports provided by the reporting tool, the only report relevant to this assessment is the “Host Report” which lists the top 100 IP addresses based on the number of requests for pages.

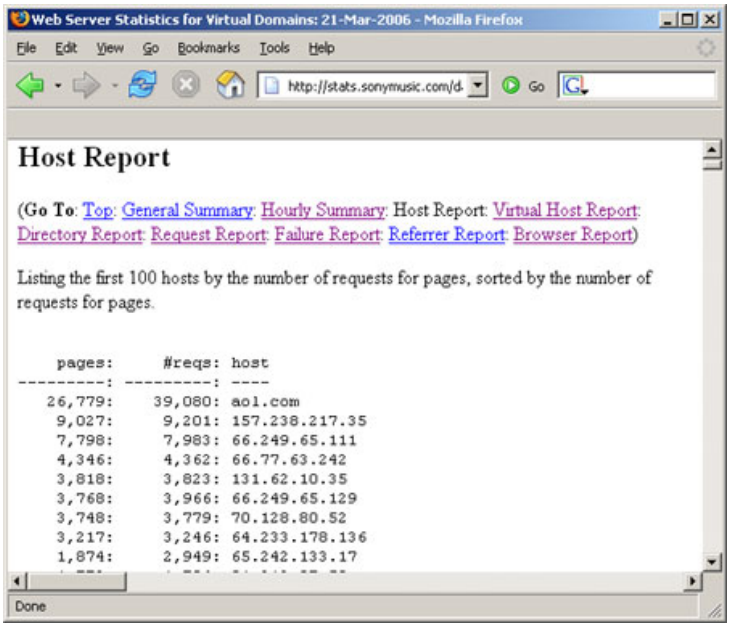


Figure 4-8

The “Host Report” provides IP address alone, and a review of the full contents of the reporting tool confirmed that the tool does not aggregate and / or correlate information from web logs in a manner that would enable SONY BMG to associate personally identifiable information about any user. The reports generated through this tool are retained indefinitely. Cybertrust has determined that SONY BMG does not aggregate and / or correlate information from web logs with any other data source in a manner that would enable SONY BMG to develop personally identifiable information about any user.

4.4 Server Side Privacy Assessment – MediaMax v.3 and v.5 Software

The scope of the MediaMax Server Side Privacy Assessment was limited to those SunnComm systems that facilitate the transfer or storage of data resulting from use of a MediaMax v.3 and / or MediaMax v.5 CD. Specifically, the systems considered in-scope are outlined in the figure below.

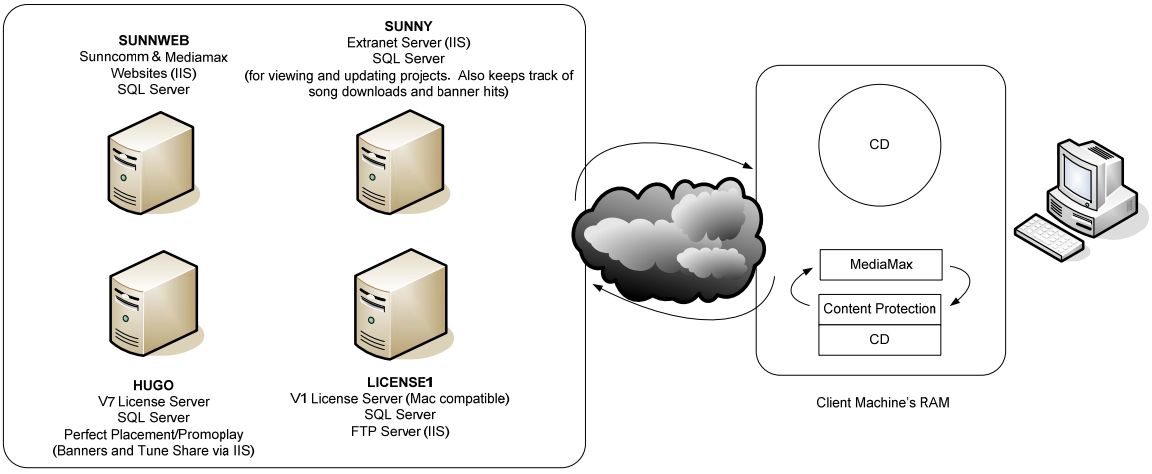


Figure 4-9

All of the servers that were considered in-scope for this assessment are dual purposed IIS web and SQL Server database servers.

From the variety of databases that sit within the four SQL Servers, personnel interviews and on-console reviews of the SunnComm servers concluded that the contents of the SQL Server databases are outside of the scope of this assessment.

The MediaMax v.3 Player and the MediaMax v.5 Player are supported by server side applications driven by Microsoft's ASP technology. Their ASP applications are hosted on Windows 2000 Server platforms on IIS 5.0 web servers.

To confirm the inbound traffic originating from MediaMax v.3 and MediaMax v.5 Players, the IIS web logs were extracted and reviewed. Cybertrust found that the logs collected by SunnComm's IIS Servers did not collect any personally identifiable data. The requests found on the SunnComm servers closely matched the requests made by the MediaMax Players during Cybertrust's test.

4.5 Server Side Privacy Assessment – SunnComm Data Retention

Interviews with SunnComm's network administrator revealed that at the time of this assessment SunnComm did not have a formal data retention policy governing the collection, storage, or destruction of data. Operationally, SunnComm's server segment is protected by a live back-up system that can make web access logs and database backups available for up to three years. SunnComm has confirmed that their data retention as it pertains to MediaMax applications does not involve purging that data. Interviews with SunnComm administrators indicates that data from the MediaMax applications existing within SunnComm's environment go back three years.

SunnComm does not use the web logs that maintain IP addresses for any type of reporting purposes. Cybertrust's on console review of SunnComm's production systems and databases confirmed that SunnComm does not aggregate and / or correlate information from the web logs in any manner that would enable SunnComm to associate personally identifiable information about any user. Additionally, Cybertrust has determined that SunnComm does not aggregate and / or correlate information with any other data sources that would enable SunnComm to associate personally identifiable information about any user.

5 Statement of Opinion

5.1 XCP

Based on Cybertrust's data privacy assessment of the XCP Software, as well as server segments that support the XCP Software, Cybertrust has determined that SONY BMG has not used the XCP Software, or any of the enhanced content on the XCP CDs, to collect, aggregate or retain personally identifiable information without user consent. Cybertrust has determined that the XCP Bundled Player transmits only certain non-personally identifiable information (album ID and IP address) to provide the Enhanced CD Functionality. Cybertrust has found that SONY BMG temporarily retains this non-personally identifiable information as part of standard web logging activities. Cybertrust has also determined that SONY BMG does not associate or aggregate that information with any other information to produce personally identifiable information.

5.2 MediaMax v.3

Based on Cybertrust's data privacy assessment of the MediaMax v.3 Software as well as the server segments that support the MediaMax v.3 Software, Cybertrust has determined that SONY BMG and SunnComm have not used the MediaMax v. 3 Software, or any of the enhanced content on the MediaMax v.3 CDs, to collect, aggregate or retain personally identifiable information without user consent. Cybertrust has determined that the MediaMax v.3 Player transmits certain non-personally identifiable information (album ID, track IDs, and IP address) to provide the Enhanced CD Functionality. Cybertrust has found that SunnComm retains this non-personally identifiable information as part of standard web logging activities. Cybertrust has determined that SunnComm does not associate or aggregate that information with any other information to produce personally identifiable information.

5.3 MediaMax v.5

Based on Cybertrust's data privacy assessment of the MediaMax v.5 Player, as well as server segments that support the MediaMax v.5 Software, Cybertrust has determined that SONY BMG and SunnComm have not used the MediaMax v.5 Software, or any of the enhanced content on the MediaMax v.5 CDs, to collect, aggregate or retain personally identifiable information without user consent. The MediaMax v.5 Software does not collect any information that can be used to personally identify a user without user consent. Cybertrust has determined that the MediaMax v.5 Player transmits certain non-personally identifiable information (album ID, track IDs, and IP address) to provide the Enhanced CD Functionality. Cybertrust has found that SunnComm retains this non-personally identifiable information as part of standard web logging activities. Cybertrust has determined that SunnComm does not associate or aggregate that information with any other information.

Based on Cybertrust's findings, it is Cybertrust's opinion that the SONY BMG Representations are accurate: SONY BMG has not used the MediaMax or XCP Software, or any enhanced content on XCP CDs or MediaMax CDs, to collect, aggregate, or retain Personal Data about individuals who listened to XCP CDs or MediaMax CDs on computers, without such person's express consent.

Appendix 1 – Client Side Testing Program

Introduction

This portion of the document outlines the testing methodology and programs employed by Cybertrust to determine if SONY BMG has collected, aggregated, or retained Personal Data in a manner that is inconsistent with the SONY BMG Representations.

Test Scenarios

The following scenarios were developed to assess the operation of the XCP Bundled, MediaMax v.3, and MediaMax v.5 Players on a user's computer.

A base image was used to maintain a standard testing environment throughout the test scenarios within this appendix. The image was captured and deployed onto the physical test host using Symantec Ghost Version 8.0.0.984. The base image, as described bellow will be referred to throughout the rest of this testing document as the "vanilla image."

The base testing platform that was used throughout the duration of the test constituted:

Dell Inspiron 2650 1.19 GHz Pentium 4 w/ 256 MB of RAM

- OS
  - Windows XP Professional Version 2002 Service Pack 1
- Applications
  - Flash Player 8.0.24.0 (Configured to work with MediaMax)
- Browser
  - Internet Explorer Version 6.0.2800.1106.xpsp1.020828-1920
- Media Player
  - Windows Media Player Version 10.00.00.3802
- Packet Analysis
  - Ethereal – Network Protocol Analyzer Version 0.10.12 w/ WinPcap version 3.1 beta4

Common sections throughout the testing document will be:

- Entry: Information within this section should be read and considered going into each testing scenario.
- Execution: Information within this section will be helpful in aiding the tester to properly execute a test.
- Exit: This section quantifies any post test requirements that may need to be met prior to the tester moving on to the next scenario.

Each individual scenario is comprised of:

- Scenario: outlines the event or condition that will be tested.
- Expected Event: specifies the event(s) that the tester should see while the described scenario is executed.

- Recorded Data Transfer: presents the relevant events, recorded by the tester that took place, as the scenario was being executed.

XCP

Entry:

- Begin with the vanilla image restored onto the test host.
- Configure Ethereal with the following settings:
  - INPROCOMM IPN2220 Wireless LAN Adapter
  - IP Address: 192.168.0.5
  - Buffer size: 1 MB
  - Update list of packets in real time: Yes
  - Automatic scrolling in live capture: Yes
  - Enable network name resolution: Yes
  - Enable transport name resolution: Yes

Scenario 1: Tester loads XCP CD into the test host which is connected to the Internet.

- Expected Event
  - The XCP Bundled Player presents the EULA to the tester.
  - The content protection software is installed.
  - The XCP Player application initiates a communication with SONY BMG servers to pull down the banner content for a particular artist. The XCP Bundled Player loads with a banner which rotates.
- Recorded Data Transfer
  - The XCP Bundled Player makes a call out to connected.sonymusic.com, specifically contacting the TOC application and looking for the redirect associated with the uId=1198, tied to Patty Loveless.
  - The connected.sonymusic.com server sends a response back to the XCP Bundled Player letting the client know that the file that it's looking for is located on the xcpimages.sonybmg.com server, specifically within the XML virtual directory.
  - The XCP Bundled Player follows the redirect provided by connected.sonymusic.com and makes a call out to xcpimages.sonybmg.com/xml/pattyloveless.xml and pulls back an XML file that specifies:
    - **Banner src**: The source of the banner jpg file
    - **Href**: The link that a web browser would be sent it if the specific banner jpg file is clicked
    - **Time**: The length of time the banner should be displayed on the XCP Bundled Player

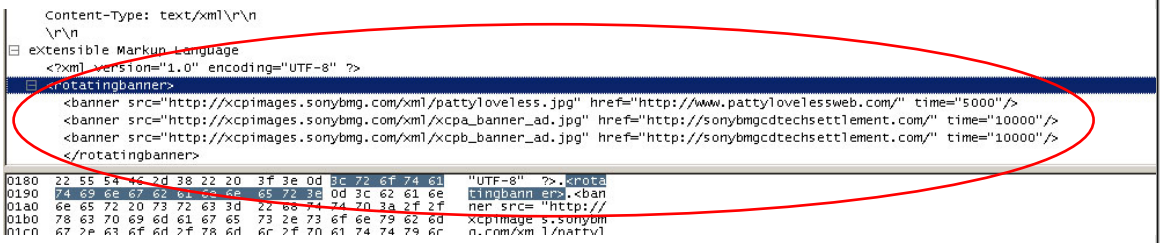


Figure A-1

- With the XML file pulled down from the xcpimages.sony.com server the XCP Bundled Player pulls the graphics required to render the banners specified by the XML banner file.

- The first file that gets pulled down is the pattyloveless.jpg file from the xcpimages.sonybmg.com site: GET / xml/pattyloveless.jpg HTTP 1.0.

Figure A-2

- The second file that gets pulled down is the xcpa_banner_ad.jpg file from the xcpimages.sonybmg.com site: GET /xml/xcpa_banner_ad.jpg HTTP 1.0.

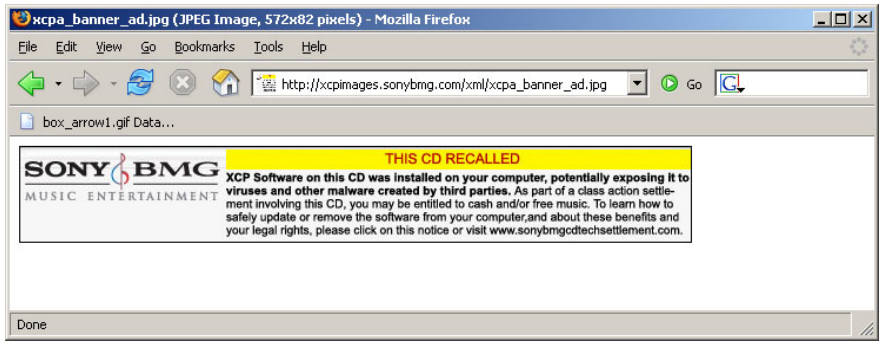


Figure A-3

- The third file that gets pulled down is the xcpb_banner_ad.jpg file from the xcpimages.sonybmg.com site: GET /xml/xcpb_banner_ad.jpg HTTP 1.0.

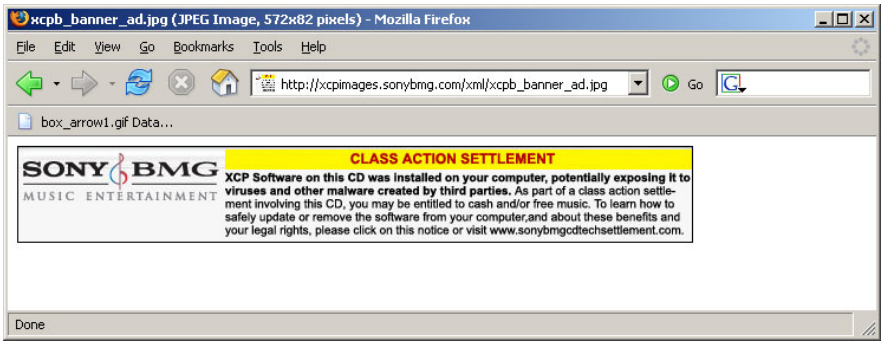


Figure A-4

Scenario 2: Allow the CD to run for the length of the entire album with Ethereal continuing to capture packets.

- Expected Event
  - The XCP Bundled Player plays through the rest of the CD.
- Recorded Data Transfer
  - Following the XCP Bundled Player's download of the banner xml file and the associated graphics, the XCP Bundled Player was used to play through the entire contents of the CD after which the XCP Bundled Player was left on for a total run time of 60 minutes. The packet analysis revealed that the XCP Bundled Player made no additional attempts to communicate on the network. The packet analysis confirmed that all other traffic identified by the packet capture was associated with infrastructure and system traffic with no ties to the XCP Bundled Player.

Scenario 3: Test the links in the main XCP Bundled Player page.

- 3[a] Click the "Patty Loveless Dreamin' My Dreams" icon on the top left corner of the XCP Bundled Player window.
  - Expected Event
    - The XCP Bundled Player opens a web browser and redirects the browser to www.pattylovelessweb.com.
  - Recorded Data Transfer
    - The XCP Bundled Player sends an outbound request to connected.sonymusic.com, searching for the redirect associated with the uId=1187.
    - The XCP Bundled Player receives a response back that instructs it to redirect the browser to www.pattylovelessweb.com.
    - The packet analysis shows the traffic associated with loading the www.pattylovelessweb.com site on the test system's web browser.

Exit: Close the popped up web browser and return to the XCP Bundled Player's main page by clicking the "Music" icon located in the top left corner of the Player.

- 3[b] Click the "Music" link on the top left corner of the XCP Bundled application, located directly under the "Patty Loveless" link.
  - Expected Event
    - The "music" link is a reference to the home page of the XCP Bundled application and clicking the link should send the user to the home page of the application. If the user is already on the home page, clicking the link should have no effect on the system.
  - Recorded Data Transfer:
    - The packet analysis showed no network communications of any type associated with the XCP Bundled Player when the "Music" link on the top left corner of the XCP Bundled application was clicked.

- 3[c] Click the "Epic" icon on the top right corner of the XCP Bundled Player window.
  - Expected Event
    - The XCP Bundled Player opens a web browser and redirects the browser to www.epicrecords.com.
  - Recorded Data Transfer
    - The XCP Bundled Player sends a request to connected.sonymusic.com for a redirect with the client provided uId=1199.
    - The XCP Bundled Player receives back a redirect to www.epicrecords.com in the form of a HTTP 302 server response.

- The packet analysis shows the traffic associated with loading the www.epcirecords.com site on the test system's web browser.

Exit: Close the popped up web browser and return to the XCP Bundled Player's main page by clicking the "Music" icon located in the top left corner of the Player.

- 3[d] Click the "Sony Music Nashville" icon on the top right corner of the XCP Bundled Player window.
  - Expected Event
    - The XCP Bundled Player opens a web browser and redirects the browser to www.sonynashville.com.
  - Recorded Data Transfer
    - The XCP Bundled Player sends a request to connected.sonymusic.com for a redirect with the client provided uId=1204.
    - The XCP Bundled Player receives back a redirect to www.sonynashville.com in the form of a HTTP 302 server code.
    - The packet analysis shows the traffic associated with loading the www.sonynashville.com site on the test system's web browser.

Exit: Close the popped up web browser and return to the XCP Bundled Player's main page by clicking the "Music" icon located in the top left corner of the Player.

- 3[e] Click the "?" icon on the top right corner of the XCP Bundled Player window.
  - Expected Event
    - The XCP Bundled Player opens a web browser and redirects the browser to a readme.html located in the root directory of the XCP CD.
  - Recorded Data Transfer
    - As expected the packet analysis showed no network communications of any type associated to the XCP Bundled Player when the "?" link on the top right corner of the XCP Bundled Player was clicked.

Exit: Close the popped up web browser and return to the XCP Bundled Player's main page by clicking the "Music" icon located in the top left corner of the Player.

- 3[f] Click the "This CD Recalled" banner on the bottom of the XCP Bundled Player window.
  - Expected Event
    - The XCP Bundled Player opens a web browser and redirects the browser to sonybmgcdtechsettlement.com.
  - Recorded Data Transfer
    - When the "This CD Recalled" banner was clicked the XCP Bundled Player opened a web browser and redirected the web browser to sonybmgcdtechsettlement.com.
    - The packet analysis shows the traffic associated with loading the sonybmgcdtechsettlement.com site on the test system's web browser.

Exit: Close the popped up web browser and return to the XCP Bundled Player's main page by clicking the "Music" icon located in the top left corner of the Player.

- 3[g] Click the "Class Action Settlement" banner on the bottom of the XCP Bundled Player window
  - Expected Event

        - The XCP Bundled Player opens a web browser and redirects the browser to sonybmgcdtechsettlement.com.
    - Recorded Data Transfer
        - When the "Class Action Settlement" banner was clicked the XCP Bundled Player opened a web browser and redirected the web browser to sonybmgcdtechsettlement.com.
        - The packet analysis shows the traffic associated with loading the sonybmgcdtechsettlement.com site on the test system's web browser.

Exit: Close the popped up web browser and return to the XCP Bundled Player's main page by clicking the "Music" icon located in the top left corner of the Player.

- 3[h] Click the "Patty Loveless" banner on the bottom of the XCP Bundled Player window
    - Expected Event
        - The XCP Bundled Player opens a web browser and redirects the browser to www.pattylovelessweb.com.
    - Recorded Data Transfer
        - When the "Patty Loveless" banner was clicked the XCP Bundled Player opened a web browser and redirected the web browser to www.pattyloveless.com.
        - The packet analysis shows the traffic associated with loading the www.pattyloveless.com site on the test system's web browser.

Exit: Close the popped up web browser and return to the XCP Bundled Player's main page by clicking the "Music" icon located in the top left corner of the Player.

- 3[i] Click the "X" icon on the top right corner of the XCP Bundled Player window.
    - Expected Event
        - The player closes and there is no additional transfer of data from or to the XCP Bundled application between the client machine and any external party.
    - Recorded Data Transfer
        - The packet analysis showed no network communications of any type associated to the XCP Bundled Player when the "?" link on the top right corner of the XCP Bundled Player was clicked.

Entry: Reinitialize the XCP Bundled application by accessing the CDrom drive.

Scenario 4: Rip copies of the contents of the CD to the hard drive of the test system.

- 4[a] Click on the content ripping icon located on the left edge or top right corner of the XCP Bundled Player. From the CD ripping page, click the "Windows Media" link, ripping full contents to the default directory.
    - Expected Event
        - The XCP Bundled Player checks the version of DirectX installed on the test system and suggests the client be upgraded.
        - The XCP Bundled Player provides a chance for the user to select a custom directory to which the media can be copied
        - The XCP Bundled Player presents the list of songs that are available for ripping, and once the tester clicks "Copy Selected Tracks" the Bundled Player copies the content to the specified directory.
    - Recorded Data Transfer

- The XCP Bundled Player makes a call out to connected.sonymusic.com, specifically contacting the TOC application and looking for the redirect associated with the uId=1198, tied to Patty Loveless.
- The connected.sonymusic.com server sends a response back to the XCP Bundled Player letting the client know that the file for which it is looking is located on the xcpimages.sonybmg.com server, specifically within the XML virtual directory.
- The XCP Bundled Player follows the redirect provided by connected.sonymusic.com and makes a call out to xcpimages.sonybmg.com/xml/pattyloveless.xml and pulls back an XML file that specifies:
  - **Banner src**: The source of the banner jpg file
  - **href**: The link that a web browser would be sent it if the specific banner jpg file is clicked
  - **Time**: The length of time the banner should be displayed on the XCP Bundled Player
- The packet analysis additionally shows traffic tied to Microsoft's Media Player pulling content but no signs of the XCP Player facilitating the transfer of any information aside from the uId tied to the album.

- 4[b] From the CD ripping page, click the "ATRAC" link
  - Expected Event
    - Window will popup and prompt tester to install Music Player
    - Music Player installer begins and deployed Music Player package (default settings / US locale)
    - Application Requires Reboot w/ CD in cdrom
  - Recorded Data Transfer
    - The packet analysis showed no network communications of any type associated to the XCP Bundled Player when the "ATRAC" link was clicked.

Entry: Open up the CD ripping page and begin the packet capture.

- 4[c] From the XCP Bundled Player's home page, navigate to the CD ripping page. Click the "ATRAC" link.
  - Expected Event
    - The XCP Bundled Player will open the Music Player application to facilitate the content extraction.
    - Rip the full contents of the CD
  - Recorded Data Transfer:
    - Packet analysis showed an outbound GET request to update.openmg.com/MUSIC_PLAYER/windows/update.inf.
    - The response back from the openmg.com site was www.openmg.com/MUSIC_PLAYER/update/&s.

Exit: Close the popped up web browser and return to the XCP Bundled Player's CD ripping page by clicking the CD ripping icon located in the top left corner of the Player.

Scenario 5: Test the links in the CD ripping page.

- 5[a] From the CD ripping page, click the "Go online to read more information about ATRAC" link
  - Expected Event

        - The XCP Bundled Player opens a web browser and redirects the browser to www.sony.net/Products/ATRAC3/
    - Recorded Data Transfer
        - The XCP Bundled Player sends an outbound request to connected.sonymusic.com, searching for the redirect associated with the uId=1182.
        - The XCP Bundled Player receives a response back that instructs it to redirect the browser to www.sony.net/Products/ATRAC3/ on the test system's web browser.

Exit: Close the popped up web browser and return to the XCP Bundled Player's CD ripping page by clicking the CD ripping icon located in the top left corner of the Player.

- 5[b] From the CD ripping page, click the "Go online to read more information about PlaysForSure" link
    - Expected Event
        - The XCP Bundled Player opens a web browser and redirects the browser to www.microsoft.com/windows/windowsmedia/devices/default.mspx
    - Recorded Data Transfer
        - The XCP Bundled Player sends a request to connected.sonymusic.com for a redirect with the client provided uId=1183.
        - The XCP Bundled Player receives back a redirect to www.microsoft.com/windows/windowsmedia/devices/ in the form of a HTTP 302 server response.
        - The packet analysis shows the entire contents of the www.microsoft.com/windows/windowsmedia/devices/ site being pulled down to the test machine to render it on the web browser.

Exit: Close the popped up web browser and return to the XCP Bundled Player's CD ripping page by clicking the CD ripping icon located in the top left corner of the Player.

- 5[c] From the CD ripping page, click the "Questions? Click here to go online and visit our help site" link
    - Expected Event
        - The XCP Bundled Player opens a web browser and redirects the browser to cp.sonybmg.com/xcp/
    - Recorded Data Transfer
        - The XCP Bundled Player sends a request to connected.sonymusic.com for a redirect with the client provided uId=1184.
        - The XCP Bundled Player receives back a redirect to cp.sonybmg.com/xcp in the form of a HTTP 302 server response.
        - The packet analysis shows the entire contents of the cp.sonybmg.com/xcp site being pulled down to the test machine to render it on the web browser.

Exit: Close the popped up web browser

Scenario 6: Burn the max number of copies of the CD.

- 6[a] From the main XCP Bundled Player page, click the CD Burning icon on the top right corner or the lower left hand corner of the player
    - Expected Event

        - The XCP Bundled Player redirects itself to a “Burn CD” window that warns the end user of the limitations set on burning the CD and prompts the tester to click a button that closes the player and opens a “Mini Burner”.
    - Recorded Data Transfer
        - The XCP Bundled Player makes a call out to connected.sonymusic.com, specifically contacting the TOC application and looking for the redirect associated with the uId=1198, tied to Patty Loveless.
        - The connected.sonymusic.com server sends a response back to the XCP Bundled Player letting the client know that the file that it is looking for is located on the xcpimages.sonybmg.com server, specifically within the XML virtual directory.
        - The XCP Bundled Player follows the redirect provided by connected.sonymusic.com and makes a call out to xcpimages.sonybmg.com/xml/pattyloveless.xml and pulls back an XML file that specifies:
            - **Banner src**: The source of the banner jpg file
            - **href**: The link that a web browser would be sent it if the specific banner jpg file is clicked
            - **Time**: The length of time the banner should be displayed on the XCP Bundled Player

- 6[b] From the “Mini Burner” Click the “OK” button
    - Expected Event
        - The Mini Burner application creates an image of the CD and ejects the burned CD.
    - Recorded Data Transfer
        - The packet analysis showed no network communications of any type associated to the XCP Bundled Player when the Mini Burner was used to create an image of the CD.

Exit: Repeat the burn two additional times to max out the burn count.

Scenario 7: Attempt to burn another copy of the CD in excess of the allowed maximum.

- From the main XCP Bundled Player page, click the CD Burning Icon on the top right corner or the lower left hand corner of the player
    - Expected Event
        - The XCP Bundled Player redirects the tester to the Mini Burner, which presents the “Unauthorized Disk Creation” error message.
    - Recorded Data Transfer
        - The packet analysis showed no network communications of any type associated to the XCP Bundled Player when the Mini Burner was used to create an image of the CD.

MediaMax v.3

Entry:

- Begin with the vanilla image restored onto the test host.
- Configure Ethereal with the following settings:
  - INPROCOMM IPN2220 Wireless LAN Adapter
  - IP Address: 192.168.0.5
  - Buffer size: 1 MB
  - Update list of packets in real time: Yes
  - Automatic scrolling in live capture: Yes
  - Enable network name resolution: Yes
  - Enable transport name resolution: Yes

Scenario 1: Tester loads MediaMax v.3 CD into a test host connected to the Internet.

- Expected Event
  - The MediaMax Player prompts the user to accept the EULA and pulls license information from the CD to the client system for the content on the CD and plays the first track of the album.
- Recorded Data Transfer
  - As the MediaMax v.3 CD is loaded into the test host the MediaMax v.3 Player makes a call out to license.sunncomm2.com, specifically to the perfectplacement virtual directory, looking for the online.asp page. The outbound request involves a query string "tm=1142451905993".
  - The MediaMax v.3 Player receives a string response back from the SunnComm server that reads "online=true&timing=3000&view=2".

Scenario 2: Allow the CD to run for the length of the entire album with Ethereal continuing to capture packets.

- Expected Event
  - The MediaMax v.3 Player plays through the rest of the CD.
- Recorded Data Transfer
  - The packet analysis showed no network communications of any type associated to the MediaMax v.3 Player as the remainder of the content on the CD was played.

Scenario 3: Test the links in the main "Welcome" MediaMax v.3 Player page.

- 3[a] Click the "RCA" icon on the bottom left side of the MediaMax player.
  - Expected Event
    - The MediaMax v.3 Player opens a web browser and redirects the browser to www.rcarecords.com.
  - Recorded Data Transfer
    - The MediaMax v.3 Player submits a HTTP GET request for www.rcarecords.com.
    - The packet analysis shows the entire contents of the www.rcarecords.com site being pulled down to the test machine to render it on the web browser.

Exit: Close the popped up web browser and return the MediaMax v.3 Player to its main page by clicking the "Welcome" link located in the top menu bar.

- 3[b] Click the “Portable device concerns? Please click here” link located in the lower right hand corner of the MediaMax v.3 Player.
    - Expected Event
        - The MediaMax v.3 Player opens a web browser and redirects the browser to www.sunncomm.com/support/portabledevice.asp.
    - Recorded Data Transfer
        - The MediaMax v.3 Player submits a HTTP GET request for www.sunncomm.com/support /portabledevice.asp.
        - The packet analysis shows the contents of the www.sunncomm.com/support/portabledevice.asp page being pulled down to the test machine to render it on the web browser.

Exit: Close the popped up web browser and return the MediaMax v.3 Player to its main page by clicking the “Welcome” link located in the top menu bar.

- 3[c] Click the “If your music does not play using your preferred player, please click here” link located in the lower right hand corner of the MediaMax v.3 Player
    - Expected Event
        - The MediaMax v.3 application redirects to an instructional page that states “You are currently enjoying your music on your PC using the original CD. Enjoying your music on ‘your computer, your way’ is easy and requires only a few steps. Use the ‘copy songs’ button to place a copy of the music on your computer. Your music will then be accessible using your preferred music player. If your music does not play using your preferred player, please click here”
    - Recorded Data Transfer
        - The packet analysis showed no network communication of any type associated with the MediaMax v.3 Player when the “if your music does not play using your preferred player, please click here” link located in the lower right hand corner of the MediaMax v.3 Player is clicked.

Exit: Return the MediaMax v.3 Player to its main page by clicking the “Welcome” link located in the top menu bar.

- 3[d] From the “Welcome” page, click the “Copy Songs” link located on the top menu bar of the MediaMax v.3 application.
    - Expected Event
        - The MediaMax v.3 application redirects to the “Copy Songs” page, which begins with “Select songs to download” and lists the different tracks within the album.
    - Recorded Data Transfer
        - The packet analysis showed no network communication of any type associated with the MediaMax v.3. Player when the “Copy Songs” link located on the top menu bar of the MediaMax v.3 application was clicked.

Exit: Return the MediaMax v.3 Player to its main page by clicking the “Welcome” link located in the top menu bar.

- 3[e] From the “Welcome” page, click the “customer care” link located on the top menu bar of the MediaMax v.3 application.
    - Expected Event

- The MediaMax v.3 Player opens a web browser and redirects the browser to www.sunncomm.com/support/faq/

o Recorded Data Transfer

- When the "customer care" link is clicked, the MediaMax v.3 Player sends a HTTP GET request for /support/sonybmg from www.sunncomm.com. The request automatically redirects to www.sunncomm.com/support/faq.
- The packet analysis shows the entire contents of the www.sunncomm.com/support/faq page being pulled down to the test machine to be rendered on the web browser opened by the MediaMax v.3 Player.

Exit: Close the popped up web browser and return the MediaMax v.3 Player to its main page by clicking the "Welcome" link located in the top menu bar.

- 3[f] From the "Welcome" page, click the "website" link located on the top menu bar of the MediaMax v.3 application.
  - o Expected Event
    - The MediaMax v.3 Player opens a web browser and redirects the browser to www.davematthewsband.com
  - o Recorded Data Transfer
    - When the "website" link is clicked, the MediaMax v.3 Player sends a HTTP GET request for www.davemathewsband.com.
    - The packet analysis shows the contents of www.davemathewsband.com being pulled down to the test machine to be rendered on the web browser.

Exit: Close the popped up web browser and return the MediaMax v.3 Player to its main page by clicking the "Welcome" link located in the top menu bar.

- 3[g] Click the "X" icon in the top right corner of the MediaMax v.3 Player
  - o Expected Event
    - The MediaMax v.3 Player shuts down.
  - o Recorded Data Transfer
    - The packet analysis showed no network communications of any type associated to the MediaMax v.3 Player when the "X" icon on the top right corner of the MediaMax v.3 Player was clicked.

Entry: Reinitialize the MediaMax v.3 Player by accessing the CDrom drive. Accept the EULA.

Scenario 4: Test the manual license pulling capabilities in the "If your music does not play using your preferred player, please click here" link, found on the bottom right corner of the MediaMax v3 application's "Welcome" page.

- From the "Welcome" page, click the "if your music does not play using your preferred player, please click here" link
- Click the "here" link embedded in the last line of the redirected page within the MediaMax v.3 application. ("If your music does not play using your preferred player, please click here")
- Click the "here" link embedded in the last line of the redirected page within the MediaMax v.3 application. ("Click here to obtain a license online.")
  - o Expected Event
    - MediaMax v.3 Player makes a connection to the Internet and pulls license keys.
    - A Windows Media Player alert will pop asking if you want to open the web page to obtain the license. Yes (you hear the bell).

- After the license information is pulled the player is returned to the welcome screen and the first track is played.

o Recorded Data Transfer

- When the manual license pull is initiated, the MediaMax v.3 Player makes an outbound HTTP GET request to license.sunncomm2.com for /perfectplacement/online.asp?tm=1142463153376, and receives back the response “online=true&timing=10000&view=1”.
- Additionally, Windows-Media-DRM makes two outbound requests to license.sunncomm2.com, which receive a total of 16 “<LICENSERESPONSE>” responses back:

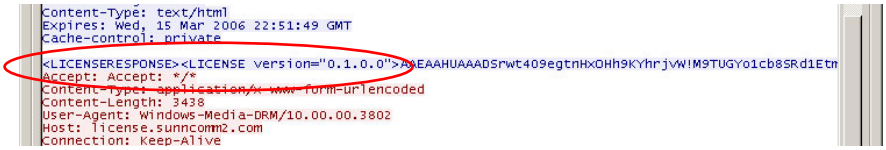


Figure A-5

- The MediaMax v.3 Player then makes a call out to the chk_license1.asp page within license1.sunncomm2.com and receives a response “license1=yes”.

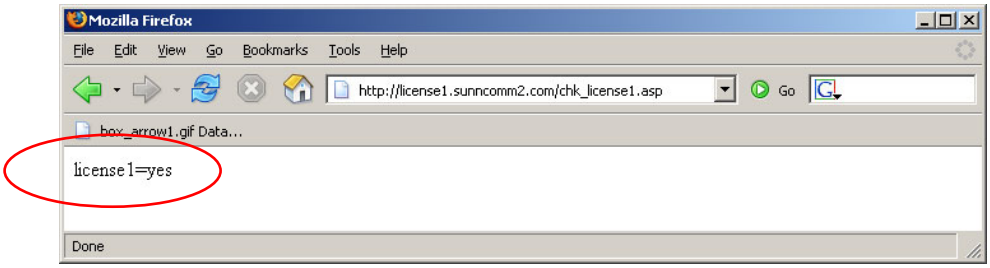


Figure A-6

- The MediaMax v.3 Player also makes an attempt to contact the license1.sunncomm2.com/chk_sunncomm.asp page and receives back a HTTP 404 Object Not Found error.

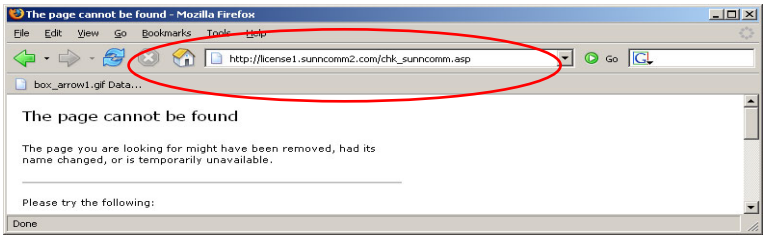


Figure A-7

Entry: Return the MediaMax v.3 Player to its main page by clicking the “Welcome” link located in the top menu bar.

Scenario 5: With the license information already pulled, attempt to pull another set of license information.

- From the "Welcome" page, click the "if your music does not play using your preferred player, please click here" link
- Click the "here" link embedded in the last line of the redirected page within the MediaMax v.3 application. ("If your music does not play using your preferred player, please click here")
- Click the "here" link embedded in the last line of the redirected page within the MediaMax v.3 application. ("Click here to obtain a license online.")
- The attempt to pull license keys will fail because the keys have already been pulled onto the system. Click the "click here to try again" link in the MediaMax v.3 application
    - Expected Event
        - MediaMax v.3 Player connects to the Internet and contacts SunnComm's license server.
        - MediaMax v.3 Player searches the local system's hard drive for license information and determines that keys already exist on the system, and ends the outbound communication, returning the application to the "Welcome" page.
    - Recorded Data Transfer
        - The MediaMax v.3 Player makes a call out to license.sunncomm2.com, specifically to the perfectplacement virtual directory, looking for the online.asp page. The outbound request involves a query string "tm= 1142463685471".
            - The MediaMax v.3 Player receives a string response back from the SunnComm server that reads "online=true&timing=3000&view=2".
        - The MediaMax v.3 Player also makes an attempt to contact the license1.sunncomm2.com/chk_sunncomm.asp page and receives back a HTTP 404 Object Not Found message.

Entry: Return the MediaMax v.3 Player to its main page by clicking the "Welcome" link located in the top menu bar.

Scenario 6: Rip copies of the contents of the CD to the hard drive of the test system.

- From the "Welcome" screen hit the "copy songs" link located on the top menu bar of the MediaMax v.3 application.
- From the list of songs, select all songs
- Click the "Continue" button which will show up after a song is selected
- Click the "Copy Songs" button which will show up after the "Continue" button is clicked.
- Accept the default folder location and click "Select"
- Expected Event
    - The MediaMax v.3 application will download the select songs to the local hard drive.
    - Because the license information was transferred to the system upon initial loading, there should be no connection to the Internet.
- Recorded Data Transfer
    - The packet analysis showed no network communication of any type associated with the MediaMax v.3 Player when the attempt was made to rip the contents of the CD to the hard drive of the test system.

MediaMax v.5

Entry:

- Begin with the vanilla image restored onto the test host.

- Configure Ethereal with the following settings:
  - INPROCOMM IPN2220 Wireless LAN Adapter
  - IP Address: 192.168.0.5
  - Buffer size: 1 MB
  - Update list of packets in real time: Yes
  - Automatic scrolling in live capture: Yes
  - Enable network name resolution: Yes
  - Enable transport name resolution: Yes

Scenario 1: Tester loads MediaMax v.5 CD into a machine connected to the Internet.

- Expected Event
  - The MediaMax v.5 Player prompts the user to accept the EULA and pulls banner content from SunnComm to render to the client, and plays the first track of the album.
- Recorded Data Transfer
  - As the MediaMax v.5 CD is loaded into the test host, the MediaMax v.5 Player makes a call out to license.sunncomm2.com/perfectplacement/retrieveassets.asp, passing along the client specific ID of "id= A8BECDD7-CF5B-4398-B4CC-65AD9FD86BBF".
  - The response sent back to the MediaMax v.5 Player is an HTML form with the following data:
    - The link to a banner graphic
    - The address to direct a client who clicks on the banner
    - The amount of time to display the banner
    - The type of graphic the banner file constitutes (GIF / JPG)

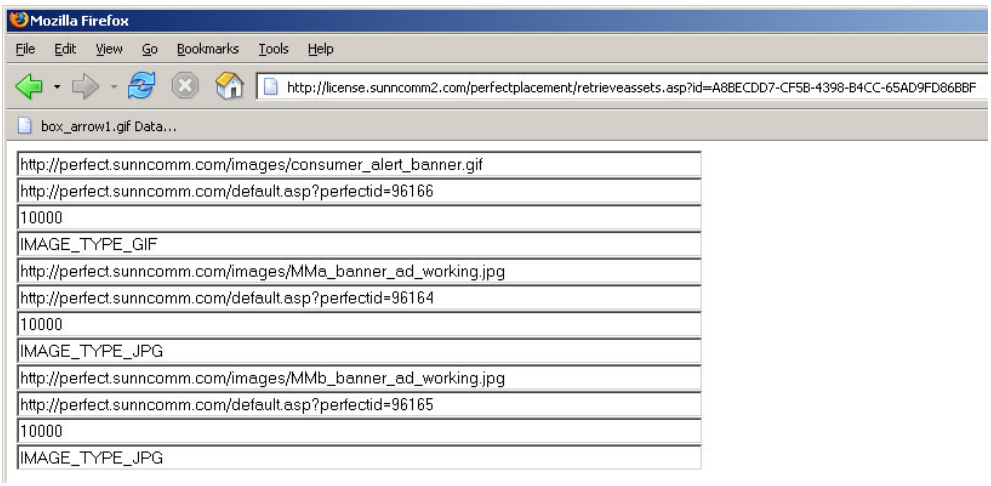


Figure A-8

  - With the banner information pulled down from license.sunncomm2.com, the MediaMax v.5 Player pulls the graphics required to render the banners specified by the HTML form.
    - The first file that gets pulled down is the consumer_alert_banner.gif from perfect.sunncomm.com.

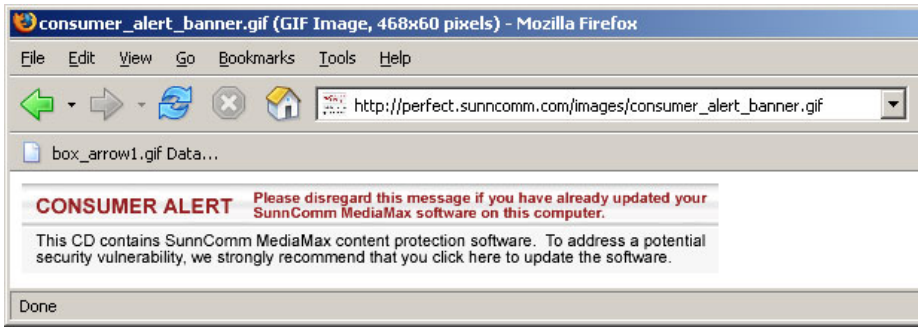


Figure A-9

- The second file that gets pulled down by the MediaMax v.5 Player from perfect.sunncomm.com is the MMa_banner_ad_working.jpg.
- The third file that is pulled down from perfect.sunncomm.com is the MMb_banner_ad_working.jpg.

Scenario 2: Run the CD for the length of the entire album.

- Expected Event
  - The MediaMax v.5 Player plays through the rest of the CD.
- Recorded Data Transfer
  - Following the MediaMax v.5 Player's download of the banner HTML form file and the associated graphics, the MediaMax v.5 Player was used to play through the entire contents of the CD after which the MediaMax v.5 Player was left on for a total run time of 70 minutes. The packet analysis revealed that the MediaMax v.5 Player made no additional attempts to communicate on the network. The packet analysis confirmed that all other traffic identified by the packet capture was associated with infrastructure and system traffic with no ties to the MediaMax v.5 Player.

Scenario 3: Test the links in the main "Home" MediaMax v.5 Player page.

- 3[a] Click the "Copy to CD" link within the top left menu bar
  - Expected Event
    - CD burning module opens.
  - Recorded Data Transfer
    - The packet analysis showed no network communications of any type associated with the MediaMax v.5 Player when the "Copy to CD" link was clicked.

Exit: Return the MediaMax v.5 Player to its main page by clicking the "Home" link located in the top left menu bar.

- 3[b] Click the "Copy to PC" link within the top left menu bar
  - Expected Event
    - CD copy module opens.
  - Recorded Data Transfer
    - The packet analysis showed no network communications of any type associated with the MediaMax v.5 Player when the "Copy to PC" link was clicked.

Exit: Return the MediaMax v.5 Player to its main page by clicking the "Home" link located in the top left menu bar.

- 3[c] Click the “Customer Care” link within the top left menu bar
  - Expected Event
    - The “Help Page and FAQ” module opens.
  - Recorded Data Transfer
    - The packet analysis showed no network communications of any type associated with the MediaMax v.5 Player when the “Customer Care” link was clicked.

Exit: Return the MediaMax v.5 Player to its main page by clicking the “Home” link located in the top left menu bar.

- 3[d] Click the “Online Support” link within the “Customer Care” module.
  - Expected Event
    - The MediaMax v.5 Player opens a web browser and redirects the browser to www.sunncomm.com/support/sonybmg, which redirects to www.sunncomm.com/support/faq.
  - Recorded Data Transfer
    - The packet analysis revealed that clicking the “Online Support” link triggered a HTTP GET request for www.sunncomm.com/support/sonybmg which received an IIS response code 302 Object moved with a redirect to www.sunncomm.com/support/faq .
    - The packet analysis details the contents of the www.sunncomm.com/support/faq page being pulled down to the test host for rendering on the web browser.

Exit: Close the web browser and return the MediaMax v.5 Player to its main page by clicking the “Home” link located in the top left menu bar.

- 3[e] Click the “Biography” link within the top left menu bar
  - Expected Event
    - The static biography content is loaded.
  - Recorded Data Transfer
    - The packet analysis showed no network communications of any type associated with the MediaMax v.5 Player when the “Biography” link was clicked.

Exit: Return the MediaMax v.5 Player to its main page by clicking the “Home” link located in the top left menu bar.

- 3[f] Click the “Artist Website” link within the top left menu bar
  - Expected Event
    - The MediaMax v.5 Player opens a web browser which is redirected to www.theloveexperience.com/index_main.html.
  - Recorded Data Transfer
    - When the “Artist Website” link is clicked, the MediaMax v.5 Player sends a HTTP GET request for www.theloveexperience.com.
    - The packet analysis shows the contents of the www.theloveexperience.com site being pulled down to the test machine to be rendered on the web browser opened by the MediaMax v.5 Player.

Exit: Close the popped up web browser and return the MediaMax v.5 Player to its main page by clicking the “Home” link located in the top left menu bar.

- 3[g] Click the “Jive” icon located in the bottom right hand corner of the MediaMax v.5 Player page.
  - Expected Event
    - The MediaMax v.5 Player opens a web browser which is redirected to www.jiverecords.com which is redirected to www.zombalabelgroup.com.
  - Recorded Data Transfer
    - When the “Jive” icon is clicked, the MediaMax v.5 Player sends a HTTP GET request for www.jiverecords.com. The browser is redirected to www.zobalablegroup.com.
    - The packet analysis shows the contents of www.zobalabelgroup.com being pulled down to the test machine to be rendered on the web browser.

Exit: Close the popped up web browser and return the MediaMax v.5 Player to its main page by clicking the “Home” link located in the top left menu bar.

- 3[h] Click the “Important Software Update” banner on the bottom of the MediaMax v.5 Player
  - Expected Event
    - The MediaMax v.5 Player opens a web browser which is redirected to www.sonybmgcdtechsettlement.com.
  - Recorded Data Transfer
    - When the “Important Software Update” banner is clicked, the MediaMax v.5 Player sends a HTP GET request for perfect.sunncomm.com/default.asp?pefectid=96165. The response sent back to the web browser is a HTTP 302 Object moved message which redirects the browser to www.sonybmgcdtechsettlement.com.
    - The packet analysis shows the contents of www.sonybmgcdtechsettlement.com being pulled down to the test machine to be rendered on the web browser.

Exit: Close the popped up web browser and return the MediaMax v.5 Player to its main page by clicking the “Home” link located in the top left menu bar.

- 3[i] Click the “Class Action Settlement” banner on the bottom of the MediaMax v.5 Player
  - Expected Event
    - The MediaMax v.5 Player opens a web browser which is redirected to www.sonybmgcdtechsettlement.com.
  - Recorded Data Transfer
    - When the “Class Action Settlement” banner is clicked, the MediaMax v.5 Player sends a HTTP GET request for perfect.sunncomm.com/default.asp?perfectid=96164. The response sent back to the web browser is a HTTP 302 Object moved message which redirects the browser to www.sonybmgcdtechsettlement.com.
    - The packet analysis shows the contents of www.sonybmgcdtechsettlement.com being pulled down to the test machine to be rendered on the web browser.

Exit: Close the popped up web browser and return the MediaMax v.5 Player to its main page by clicking the “Home” link located in the top left menu bar.

- 3[j] Click the “Consumer Alert” banner on the bottom of the MediaMax v.5 Player
  - Expected Event

- The MediaMax v.5 Player opens a web browser which is redirected to www.sonybmgcdtechsettlement.com.

  - Recorded Data Transfer
    - When the “Consumer Alert” banner is clicked, the MediaMax v.5 Player sends a HTTP GET request for perfect.sunncomm.com/default.asp?perfectid=96166. The response sent back to the web browser is a HTTP 302 Object moved message which redirects the browser to www.sonybmgcdtechsettlement.com.
    - The packet analysis shows the contents of www.sonybmgcdtechsettlement.com being pulled down to the test machine to be rendered on the web browser.

Exit: Close the popped up web browser and return the MediaMax v.5 Player to its main page by clicking the “Home” link located in the top left menu bar.

- 3[k] Click the “X” icon on the top right corner of the MediaMax v.5 Player
  - Expected Event
    - The player goes through the shutdown process
  - Recorded Data Transfer
    - The packet analysis showed no network communications of any type associated with the MediaMax v.5 Player when the “X” icon on the top right corner of the MediaMax v.5 Player was clicked.

Entry: Reinitialize the MediaMax v.5 Player by accessing the CDrom drive.

Scenario 4: Rip copies of the contents of the CD to the hard drive of the test system.

- From the “Home” screen hit the “Copy to PC” link within the top left menu bar.
- Click the “Begin” button located in the bottom right corner of the “Copy to PC” module.
  - Expected Event
    - The MediaMax v.5 application initiates the content rip module.
- Accept the default folder location and click “Ok”
- When asked “Would you like to add your selection to the Windows Media Player Library?” OK is clicked
  - Expected Event
    - The media is copied off of the CD onto the hard drive.
  - Recorded Data Transfer
    - The packet analysis showed no network communications of any type associated with the MediaMax v.5 Player when the contents of the CD were ripped onto the test system’s hard drive.

Exit: Close the popped up web browser and return the MediaMax v.5 Player to its main page by clicking the “Home” link located in the top left menu bar.

Scenario 5: Burn the maximum number of copies of the CD.

- From the “Home” screen of the MediaMax v.5 Player hit the “Copy to CD” link within the top left menu bar.
  - Expected Event
    - The “Copy to CD” module redirects to a device configuration page, followed by a summary page, and the actual burn process run by “SecureBurn”
  - Recorded Data Transfer

- The packet analysis showed no network communications of any type associated with the MediaMax v.5 Player when the contents of the CD were burned onto blank media.

Scenario 6: Attempt to burn another copy of the CD in excess of the allowed maximum.

- From the “Home” screen of the MediaMax v.5 Player hit the “Copy to CD” link within the top left menu bar.
  - Expected Event
    - The “Copy to CD” module raises an error
  - Recorded Data Transfer
    - The packet analysis showed no network communications of any type associated with the MediaMax v.5 Player when the attempt was made to burn a copy of the media in excess of the allowed number.